824

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,376	01/24/2002	Sami Kilkkila	602.361USW1	2033

32294 7590 11/10/2004

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/057,376	KILKKILA, SAMI	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 24 January 2002 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 01/24/2002.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (5751812) in view of Feldman et al (5862225).

With respect to Claim 1, Anderson meets the limitation of "a telecommunication network (OM); a source system (LEl) connected to the telecommunication network (OM); a target system (LE2) connected to the telecommunication network (OM)" on column 1, lines 7-12; and "storing user identifiers and associated passwords in the source system (LEl) and in the target system (LE2)" on column 2, lines 2-7. If a hash is computed using the received password at both the client and the server, the password is inherently stored in the memory of both systems during the operations to enable this computation to be possible. The seed in Fig. 4 represents the user identifier. Anderson meets further limitation of "logging on into the source system (LEl) by entering a user identifier and a password corresponding to it" on Fig. 1 and on column 1, lines 38-40; and "identifying the user in the source system (LE1); and setting up a remote session to the target system (LE2)" on column 1, lines 61-67 and on column 2, lines 1-10; and "generating identical indexed encryption keys in the source system (LEl) and in the target system (LE2); encrypting the password associated with the user identifier in the source system (LEl) using the encryption key indicated by a first index, and sending the encrypted data as well as the first index

and the user identifier to the target system (LE2)" on column 1, lines 61-67 and on column 2, lines 1-5; and "encrypting the password associated with the user identifier in the target system (LE2) using an encryption key indicated by the index received" on column 1, lines 64-66. This is because the server already stores an encrypted/hashed version of the user's password. Further limitation of "performing a first comparison between the received password and the password encrypted in the target system (LE2)" is met on column 2, lines 5-7. The hash function represents the encryption keys and has an index, i present. Anderson however does not meet the following limitation.

Feldman et al meets the limitation of "encrypting in the target system (LE2) the password received from the source system (LEl) using an encryption key indicated by a second index, and sending the encrypted data and the second index to the source system (LEl); encrypting the encrypted password initially sent from the source system (LEl) to the target system (LE2) again using the encryption key indicated by the second index received from the target system (LE2); performing a second comparison between the encrypted password received from the target system (LE2) and the password encrypted in the source system (LEl) using the encryption keys indicated by the first and second indexes" on column 2, lines 28-47; and "approving the setup of the remote session if the results of the comparisons are coincident" on column 2,lines 42-47.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Feldman et al within the system of Anderson so as to ensure a secure log-in by a user to a network. Re-encrypting the hash function is a repetition of the initial encryption of the hash function, which is already known in the art as a form of message authentication.

With respect to Claim 2, Anderson meets the limitation of "characterized in that the setup of the remote session is prevented if the results of the first or the second comparison are not coincident" on column 2, lines 7-11.

With respect to Claim 14, its limitation is similar to Claim 1 limitation and hence its rejection can be found therein.

With respect to Claim 15, Anderson meets the limitation of "characterized in that the system comprises means (6) for preventing the setup of a remote session" in the abstract.

Claims 3-13, 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (5751812) in view of Feldman et al (5862225) in further view of Akiyama et al (5784464).

With respect to Claim 3, Anderson and Feldman et al meets all the limitation except for the following limitation.

Akiyama meets the limitation of "separate identification data is generated" on column 2, lines 10-25; and "the identification data is encrypted in the source system (LEl) using the encryption key indicated by the first index and the encrypted data is sent to the target system (LE2)" on column 4, lines 34-38; and "the identification data received from the source system (LEl) is encrypted in the target system (LE2) using the encryption key indicated by the second

index and the encrypted data as well as the second index are sent back to the source system (LEl)" on column 4, lines 20-22; and "the identification data encrypted using the encryption key indicated by the first index which was initially sent to the target system (LE2) is encrypted again in the source system (LEl) using the encryption key indicated by the second index received from the target system (LE2)" on column 4, lines 22-27; and "a third comparison is performed between the encrypted identification data received from the target system (LE2) and the identification data just encrypted in the source system (LEl); and the setup of the remote session is approved if the result of the comparison is coincident" on column 4, lines 29-34.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 4, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the setup of the remote session is prevented if the result of the third comparison is not coincident" on column 4, lines 29-34.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 5, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "the identification data is sent simultaneously with the user data; or the identification data is sent in separation from the user data" on column 3, lines 6-11 and 16-20.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 6, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that time data and/or data individualizing the source system is added to the identification data" on column 1, lines 64-67.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 7, Anderson and Feldman et al meets all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the encryption keys are generated using a certain predetermined algorithm" on column 2, lines 50-56.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 8, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the encryption keys are stored on a special encryption key list" on column 2, lines 50-56.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 9, Anderson meets the limitation of "characterized in that the index is generated on a random basis or on the basis of a predetermined algorithm" on column 1, lines 41-50. The index is represented by i.

With respect to Claim 10, Anderson meets the limitation of "characterized in that a one-way encryption algorithm is used f or the encryption of data in the source system (LEI) and in the target system (LE2)" on column 2, lines 2-7.

With respect to Claim 11, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the telecommunication system is a telephone exchange system" on column 1, lines 20-22.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 12, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the source system (LEl) and/or the target system (LE2) are telephone exchanges" on column 1, lines 13-22.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 13, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the telecommunication network (OM) is an operation and maintenance network" on column 1, lines 13-22. This is because an operation and maintenance network can be categorized as a digitally distributed data over a network.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 16, Anderson and Feldman et al meet all the limitation except for the following limitation. Akiyama meets the limitation of "characterized in that the system comprises means (7) for generating identification data and adding time data and/or data individualizing the source system to the identification data" on column 1, lines 64-67.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Akiyama et al within the combination of Anderson and Feldman et al because the identification data is necessary for the authentication between the user and service provider.

With respect to Claim 17, its limitation is similar to Claim 8 limitation and hence its rejection can be found therein.

With respect to Claim 18, its limitation is similar to Claim 9 limitation and hence its rejection can be found therein.

With respect to Claim 19, its limitation is similar to Claim 11 limitation and hence its rejection can be found therein.

With respect to Claim 20, its limitation is similar to Claim 12 limitation and hence its rejection can be found therein.

With respect to Claim 21, its limitation is similar to Claim 13 limitation and hence its rejection can be found therein.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

OTA